Employment Development Department

State of California

Job Training Partnership Act Encryption/Decryption Software Users Guide

Prepared By
Job Training Partnership Division
August 1999

Job Training Partnership Act
Encryption/Decryption Software Users Guide

Table of Contents

Chapter

1

Introduction

Pretty Good Privacy (PGP) is encryption/decryption software based on a widely accepted encryption technology known as public key cryptography, in which two complementary keys are used to maintain secure communications. One of the keys is a *private key* to which only you have access and the other is a *public key* that you freely exchange with other PGP users. Both keys are stored in key-ring files, which are accessible from the PGP/keys window. It is from this window that you perform all your key management functions from this window.

To send someone a private e-mail message, you use a copy of that person's public key to encrypt the information, which only that person can decipher by using his or her private key. Conversely, when someone wants to send you encrypted mail, he or she uses a copy of your public key to encrypt the data, which only you can decipher by using a copy of your private key.

You can also use PGP to encrypt files that are stored on your computer, or to apply your signature to documents to authenticate they have not been altered. You also use your private key to sign the e-mail you send to others or to sign files to authenticate them. The recipients can then use their copy of your public key to determine if you really sent the e-mail and whether it has been altered while in transit. When someone sends you e-mail with his or her digital signature, you use a copy of his or her public key to check the digital signature and to make sure that no one has tampered with the contents.

Private Key

- Only user has access.
- Used to sign the e-mail messages and file attachments you send to others.
- Used to decrypt the messages and files other users send to you.

Public Key

- Used to send encrypted e-mail.
- Used to verify the sender's digital signatures.

More details are available through the Users Guide, which is available on your PGP compact disc (CD). Printing a copy of the guide, back-to-back, requires approximately 135 pages.

For PGP customer support, call (970) 522-2952.

System Requirements for Installing PGP Version 5.5 for Windows

1. Windows 95 or NT.
2. 8 MB RAM.
3. 15 MB hard disk space.

System Requirements for Installing PGP Version 5.5 for Macintosh

- Macintosh II or later model with 68030 or higher.
- System software 7.5.3 or later.
- 8 MB RAM.
- 10 MB hard disk space.

To Install PGP From CD

1. Start Windows (exit from all Windows programs before starting installation).
2. Insert the CD labeled *PGP Desktop Suite v1.0*.
3. Select the following options:

   (a) Desktop Suite
   (b) PGP 555
   (c) Disk 1
   (d) Setup.exe (computer with blue screen)

   Answer the questions that follow or select ***Next*.**

   1. Do *not* send your e-mail address to the default server.
   2. Do *not* register on the Internet.
   3. Do you have an existing keyring? ***No*.**
   4. ***Yes***, I want to launch PGP/keys.
   5. Yes/No, I do (not) want to view Read Me Files.

   Deselect the components that are not available on your system*. For example, if you do not have Exchange, deselect Microsoft Exchange/Outlook Plugin.*

   (e) Finish

Chapter

2

Key Generation Wizard

This chapter describes how to generate the public and private key pairs that you need to correspond with other PGP users.

1. Click ***Next.***

2. Click the ***Windows Start Button*** and then choose ***PGP/keys*** from the PGP submenu of the Programs Menu or the PGP tray. You can also open this window by clicking the ***Double Key Icon*** located in your e-mail application's toolbar then select ***New Key*** from the Keys menu.

3. Click ***Next***.

4. Enter ***your name*** on the ***first line*** and ***your e-mail address*** on the ***second line***.

5. Click ***Next***.

6. Key type: ***Diffie-Hellman/DSS (2048 bits [2048 DH/1024 DSS]).***

7. Key pair size: ***1024 bits***. Do **not** specify a size other than the default values for a Diffie-Hellman/DSS key or the fast key generation option is not used and it may take hours to generate your key.

   NOTE: When creating a Diffie-Hellman/DSS key, the size of the DSS portion of the key is increased in fixed increments less than or equal to the size of the Diffie-Hellman portion of the key, and is limited to a maximum size of 1024 bits.

8. Click ***Next***.

9. The PGP Key Generation Wizard asks you to indicate when the key pair should expire. Accept the default selection ***Never*****.**

10. Click ***Next***.

11. In the ***PGP Passphrase Enter Box***, enter a string of characters or words you want to use to maintain exclusive access to your private key. To confirm your entry, press the Tab key to advance to the next line, then enter the same passphrase again.

12. Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. If you would like to see your passphrase as you type, clear the ***Hide Typing Check Box***.

    TIP: Your passphrase should contain multiple words and may include spaces, numbers, and punctuation characters. Choose something you can remember easily but that others will not be able to guess. The passphrase is case sensitive, meaning that it distinguishes between uppercase and lowercase letters. Strong passphrases include uppercase and lowercase letters, numbers, punctuation, and spaces. The longer your passphrase, and the greater the variety of characters it contains, the more secure it is. Try to include some numbers or uppercase and lowercase alphabetic characters, numbers, punctuation marks, and so on.

13. The ***Quality Bar*** shows the strength of your passphrase compared to the strength of the key being generated. A full bar means that they are roughly equivalent.

14. Click ***Next***.

15. The ***PGP Key Generation Wizard*** will indicate that it is busy generating your key.

16. An inadequate passphrase will generate a warning message before the keys are generated. You have the choice of accepting the bad passphrase or entering a more secure one before continuing.

17. If there is not enough random information upon which to build the key, the ***PGP Random Data Dialog Box*** appears. Move your mouse around and enter a series of random keystrokes until the progress bar is completely filled in. Your mouse movements and keystrokes generate the random information that is needed to create a unique key pair.

    NOTE: The PGP Version 5.0 and later constantly gather random data from many sources on the system including mouse position, timing, and keystrokes. If the Random Data dialog box does not appear, the PGP has already collected all the data it needs.

18. Generating a key can take several minutes; *the* ***PGP Key Generation Wizard*** indicates that the key generation process has completed.

19. Click ***Next***.

20. The ***Key Generation Wizard*** indicates that you have successfully generated a new key pair and asks if you want to send your public key to a key server**. Do not send your public key to a key server.**

21. Specify whether you want your new public key to be sent to the appropriate key server for your domain and then click ***Next***. When you send your public key to the key server, anyone who has access to that key server can get a copy of your key when he or she needs it.

22. When the key generation process is complete, the final dialog box appears. Click ***Finish***. A pair of keys representing your newly created keys appears in the ***PGP/keys window***.

When you open the mail screen the PGP icons should be part of the toolbar. *

***NOTE: Exchange Customers**: **Word must be de-selected as your e-mail editor or the PGP icons will not appear.**

De-Select Word as E-Mail Editor

To de-select Word as your e-mail editor, do the following after opening e-mail:

1. Select ***Compose****.*

2. Select ***Word Mail Options****.*

3. At the bottom of the screen, make sure that the box next to “Enable Word as e-mail editor” is **NOT** selected.

Distributing Your Public Key

Although there are other alternatives for distributing your public key, we recommend that you send your public key in an e-mail message.

1. Prepare an e-mail message. In some e-mail applications, you can simply drag your key from the PGP/keys window into the text of your e-mail message to transfer the key information.

2. Open the PGP/keys window by clicking the ***Lock and Key icon*** in the system tray.

3. Highlight your ***Key Pair***, then choose ***Copy*** from the Edit menu.

4. Place the cursor in the desired area in your e-mail, then choose ***Paste*** from the Edit menu.

Obtaining the Public Keys of Others

If you have an e-mail application that is supported by the PGP plug-in, you can add the sender's public key to your public keyring by ***simply clicking a button***. For example, when an e-mail message arrives with a text block containing someone's public key***, click the Key and Envelope button*** to have the key stored on your public keyring.

If you are using an e-mail application that is not supported by the plug-ins, you can add the public key to the keyring by ***copying the block of text that represents the public key and pasting it into the PGP/keys window.***

Protecting Your Keys

Once you have generated a key pair, it is wise to create a spare pair and put them in a safe place in case something happens to the originals. Your private keys and your public keys are stored in separate keyring files, which you can copy just like any other files to another location on your hard drive or to a floppy disk. By default, the private keyring (***secring.skr***) and the public keyring (***pubring.pkr***) are stored along with the other program files in the PGP file directory; however, you can save your backups in *any* location.

The PGP creates backup copies of your public and private keys when they are generated. These copies are called ***pubring.pkr.bak*** and ***secring.skr.bak***. You can also store your keys on a disk. To prevent anyone else from using your key, store it on your own computer. Another alternative is to assign a different name to your private keyring, then store it somewhere **other than** in the default PGP file directory.

Disabling or Enabling a Key

- To disable a key, select ***Disable*** from the Keys menu. The key is dimmed and is temporarily unavailable for use.

- To enable a key, select the ***Enable*** from the Keys menu. The key becomes visible and can be used as before.

Deleting a Key, Signature, or User ID

1. Select the ***Key, Signature***, or ***User ID*** you want to delete.
2. Select ***Delete*** from the Edit menu.

Changing Your Passphrase

1. Select the ***Key Pair*** for which you want to change the passphrase.

2. Choose ***Key Properties*** from the Keys menu.

3. Click ***Change Passphrase***.

4. Enter your ***Old Passphrase*** in the top field of the dialog box, then press the Tab key to advance to the next field.

5. Enter your ***New Passphrase*** in the center field, then press the Tab key to advance to the bottom field.

6. Confirm your entry by ***entering your new passphrase again***.

7. Click ***OK***.

Revoking a Key

1. Select the ***Key Pair*** to revoke.

2. Choose ***Revoke*** from the key menu. A message appears with some brief information about the implications of revoking a key and asking you to specify whether you really want to revoke the selected key.

3. Click ***Yes*** to confirm your intent to revoke the selected key.

4. Enter the ***Passphrase*** in the dialog box and then click ***OK***. When you revoke a key, it is crossed out with a red line to indicate that it is no longer valid.

5. Send the revoked key to the server so everyone will know not to use your old key.

Chapter

3

The PGP/Keys Window

This chapter explains how to launch your PGP/keys window and defines PGP icon definitions.

1. Select ***Launch PGP/keys*** from the PGP pop-up menu to open PGP/keys window.

2. The PGP/keys window will display the private and public key pairs you have created for yourself as well as any public keys of other users that you have added to your public keyring.

3. From this window you create new key pairs and manage all of your other keys.

PGP Preferences

Select *PGP Preferences* from the PGP pop-up menu. The PGP preferences dialog box allows you to specify settings that affect how the PGP program functions based on your computing environment.

PGP Icon Definitions

These icons appear after PGP is installed on your system.

- LOCK ICON: Encrypts your message.

- QUILL ICON: Signs your message.

- OPENED ENVELOPE: Decrypts the message and verifies the person's digital signature.

- KEY AND ENVELOPE BUTTON: Adds any keys included in the message onto your keyring.

- DOUBLE KEYS: Double click to access the PGP/keys window. Clicking on this icon accesses the PGP/keys window at any time while composing or retrieving your mail.

- PAIR OF GOLD KEYS: Represents your Diffie-Hellman/DSS key pair, which consists of your private key and your public key.

- SINGLE GOLD KEY: Represents a Diffie-Hellman/DSS public key.

- PAIR OF BLUE KEYS: Represents your RSA key pair, which consists of your private key and your public key.

- SINGLE BLUE KEY: Represents an RSA public key.

- DIMMED KEY OR KEY PAIR: Indicates it is temporarily unavailable for encrypting and signing. You can disable a key from the PGP key window, which prevents seldom-used keys from cluttering up the Key Selection dialog box.

- KEY WITH A RED LINE THROUGH IT: Indicates that the key has been revoked. Users revoke their keys when they are no longer valid or have been compromised in some way. A key with a red X through it indicates the key that is invalid.

- KEY WITH A CLOCK: Indicates that the key has expired. A key's expiration date is established when the key is cleared.

- DIAMOND: Represents the owner of the key and lists the user names and e-mail addresses associated with the key.

- QUILL: Indicates the signatures of the PGP users who have vouched for the authenticity of the key. A signature with a red line through it indicates a revoked signature. A signature with a red X through it indicates a bad or invalid signature.

- EMPTY BAR: Indicates an invalid key or an untrusted user.

- HALF-FILLED BAR: Indicates a marginally valid key or marginally trusted user.

- FULL BAR: Indicates a completely valid key or a completely trusted user.

- STRIPED BAR: Indicates an implicitly valid key and implicitly trusted key. This setting is available only for the private and public key pairs you create.

Chapter

4

Selecting Recipients

This chapter describes how to select recipients.

If you enter a user name or e-mail address that does not correspond to any of the keys on your public keyring or if you are encrypting from the clipboard or from the Windows Explorer, you must manually select the recipient's public key from the PGP Key Selection dialog box.

To select a recipient's public key, simply drag the icon representing their key into the Recipient's list box and then click ***OK***.

Encrypting and Signing E-Mail

The procedure for encrypting and signing e-mail varies slightly between different e-mail applications. You perform the encryption and signing process by ***clicking the appropriate buttons*** on the toolbar. You can encrypt and sign your e-mail messages as well as any file attachments when you send or receive your e-mail.

If you are using an e-mail application that is not supported by the PGP plug-ins, you can encrypt and sign your e-mail messages via the Windows clipboard by selecting the appropriate option from the lock and key icon located in the system tray. To include file attachments, you encrypt the files from the Windows Explorer **before** attaching them.

TIP: If you are sending sensitive e-mail, consider leaving your subject line blank or creating a subject line that does not reveal the contents of your encrypted message.

Encrypting and Signing With Supported E-Mail Applications

When you encrypt and sign with an e-mail application that is supported by the PGP plug-ins, you have two choices depending on what type of e-mail application the recipient is using.

1. When communicating with PGP users who **have** e-mail applications that support the PGP/MIME standard, you can take advantage of a PGP/MIME feature to encrypt and sign your e-mail messages and file attachments automatically when you send them.

2. When communicating with someone who does **not** have a PGP/MIME compliant e-mail application, you should encrypt your e-mail with PGP/MIME turned off to avoid any compatibility problems. The drawback with this method is that you must separately encrypt any file attachments you want to send with the e-mail, unless you are using an application like Exchange, which allows you to encrypt and sign attachments without using PGP/MIME.

   If you do not send your e-mail immediately but instead store it in your outbox, you should be aware that when using some e-mail applications, the information is not encrypted until the e-mail is actually transmitted. Before queuing encrypted messages you should check to see if your application does in fact encrypt the messages in your outbox. If it does not, you might want to consider encrypting your messages via the clipboard before queuing them in the outbox.

Supported E-Mail Applications

1. Use your e-mail application to compose your e-mail message as you normally would.

2. When you have finished composing the text of your e-mail message, specify whether you want to encrypt and sign the text of your message by ***clicking the Lock and Quill Buttons***.

3. Send your e-mail message as normal.

4. Enter your ***Passphrase***, then click ***OK***.

5. If you have a copy of the public keys for every one of the recipients, the appropriate keys are used. However, if you specify a recipient for whom there is no corresponding public key, the ***PGP Key Selection Dialog Box*** appears so that you can specify the correct key.

6. Drag the public keys for those who are to receive a copy of the encrypted e-mail message into the “Recipients” list box. You can also double-click any of the keys to move them from one area of the screen to the other.

   NOTE: If you are not using PGP/MIME or an e-mail that does not require PGP/MIME, you must encrypt any files you want to send as attachments from the Windows Explorer before sending them.

7. Click ***OK*** to send your e-mail.

Decrypting/Verifying From Supported E-Mail Applications

1. Open your e-mail message as you normally do. You will see a block of unintelligible ciphertext in the body of your e-mail message.

2. To decrypt and verify the contents of the e-mail message, click the ***Opened Envelope Button*** on your application's toolbar.

3. Enter your ***Passphrase***, then click ***OK***. The message is decrypted. If it has been signed, a panel appears indicating whether the signature is valid.

4. After you have read the message, you can save it in its decrypted state, or you can save the original encrypted version so that it remains secure.

Chapter

5

General Preferences

This chapter describes general preferences.

Always Encrypt to Default Key — If this box is selected, all the e-mail messages and file attachments you encrypt with a "recipient" public key are also encrypted to you using your default public key.

Cache Decryption Passphrase — This setting specifies the amount of time (in hours:minutes:seconds) that your encryption passphrase is stored in your computer's memory. By default, this is set to two minutes.

Cache Signing Passphrase — This setting specifies the amount of time (in hours:minutes:seconds, e.g., 1:25:12) that your signing passphrase is stored in your computer's memory. The cache timer begins and resets every time you sign a message and erases the passphrase from memory immediately upon expiration of the timer.

Faster Key Generation — When this box is checked, less time is required to generate a new Diffie-Hellman/DSS key pair. Remember that the fast key generation is only implemented for the fixed key sizes between 1024 and 4096 provided as options when you create a key; it is not used if you enter some other values.

Display Wipe Confirmation — When this box is checked, a dialog box appears before you wipe a file to give you the last chance to change your mind before PGP securely overwrites the contents of the file and deletes it from your computer.

E-Mail Preferences

Use PGP/MIME When Sending E-Mail	When this box is checked, you do not need to explicitly turn on PGP/MIME each time you send e-mail. If you are using Eudora, and you turn this setting on, all of your e-mail messages and file attachments are automatically encrypted and signed to the intended recipient. DO NOT USE this option if you plan to send e-mail to recipients who use e-mail applications that are not supported by the PGP/MIME standard. Using Eudora, attachments are always encrypted regardless of this setting.
Word-Wrap Clear-Signed Messages at Column {}	This setting specifies the column number where a hard carriage return is used to wrap the text in your digital signature to the next line. The default setting is 70. NOTE: If you change your word-wrap setting in PGP, make sure that it is less than the word-wrap settings in your e-mail application. If you set it to be the same or a greater length, carriage returns may be added that will invalidate your PGP signature.
Encrypt New Messages by Default	Encrypts all your e-mail messages. The lock icon remains indented to indicate that the encryption function is turned on.
Sign New Messages by Default	Signs all your e-mail messages. The quill icon remains indented to indicate that the signatory function is turned on.
Automatically Decrypt When Opening Messages	Decrypts your e-mail automatically when you open a message. NOTE: This preference does not work with Eudora Version 4.0.

Quitting PGP

By default, the PGP program runs whenever you start your computer, as indicated by the lock and key icon displayed in the system tray. Select ***Quit PGP*** from the PGP pop-up menu to quit running PGP from the system tray.

Troubleshooting Pretty Good Privacy (PGP)

Error	Possible Cause	Solution
Cannot perform the requested operation because the output buffer is too small.	The output is larger than the internal buffers can handle. If you are encrypting or signing, you may have to break up the message and encrypt/sign smaller pieces at a time.	If you are decrypting or verifying, ask the sender to encrypt/sign smaller pieces and re-send them to you.
Cannot use the requested key for this operation because the key is not sufficiently trusted.	The operation cannot use a key that is not trusted.	Sign the key with your own key so that it can be trusted, then try again.
Could not encrypt to specified key because it is a sign-only key.	The selected key can only be used for signing.	Choose a different key, or generate a new key that can sign data.
Could not sign to specified key because it is a sign-only key.	The selected key can only be used for signing.	Choose a different key, or generate a new key that can encrypt data.
No secret keys could be found on your keyring.	There are no secret keys on your keyring.	Generate your pair of keys in PGP/keys.
The action could not be completed due to an invalid file operation.	The program failed to read or write data in a certain file. The file is probably corrupt.	Try altering your PGP preferences to use a different file if possible.
The specified signing key already signs this key.	You cannot sign a key that you have already signed.	You may have accidentally picked the wrong key. If so, choose a different key to sign.
The keyring contains a bad (corrupted) PGP packet. The PGP message that you are working with has been corrupted or your keyring has been corrupted.	Ask the sender to re-send the message to determine if the message has been corrupted.	Try restoring your keyring from your backup keyring.
The keyring file is corrupted.	The program failed to read or write data in a certain file. There is a file that is probably corrupt or missing. It may or may not be the keyring file.	Try using a different file name or path if possible.
The message or data contains a detached signature.	The signature for the message or file is located in a separate file.	Double-click the detached signature file first.

Troubleshooting PGP (continued)

Error	Possible Cause	Solution
The passphrase you entered does not match the passphrase on the key.	The passphrase you entered is incorrect. You may have the Caps Lock on, or you simply may have a typographical error in the passphrase.	Try again.
The PGP library has run out of memory.	The operating system has run out of memory.	Close other running programs. If that does not work, you may need more memory in your machine.
The specified key could not be found on your keyring.	The key needed to decrypt the current message is not on your keyring.	Ask the sender of the message to resend the message and make sure the sender encrypts the message to your public key.
The specified input file does not exist.	The file name typed in does not exist.	Use Windows Explorer to find the exact name and path of the file that you want.
The specified User ID was not added because it already exists on the selected key.	You cannot add a User ID to a keyring if there an identical User ID already exists on the key.	Try adding a different User ID, or delete the matching one first.
There was an error opening or writing the keyring or the output file.	A file that was needed could not be opened.	Make sure the settings in your PGP preferences are correct. If you have recently deleted files in the directory where you installed PGP, you may need to reinstall the product.
There is not enough random data currently available.	The random number generator needs more input in order to generate good random numbers.	When prompted, move the mouse around or press random keys in order to generate input.
Unable to perform operation because this file is read-only or otherwise protected.	If you store your keyring files on removable media, the media may not be inserted. A file that was needed is set to read-only or is being used by another program.	Close other programs that may be accessing the same files as the program you are running. If you keep your keyring files on a floppy, make sure that the floppy is in the floppy drive.